

Project Research Report

Home Security Threat Analysis

Luke Savage(C00248077) - 4th Year Cybercrime & IT Security





Contents

[Introduction 2](#_Toc132660985)

[Threat Analysis 2](#_Toc132660986)

[What is Threat Analysis? 2](#_Toc132660987)

[What are the benefits of Threat Analysis? 3](#_Toc132660988)

[How do you perform a Threat Analysis? 4](#_Toc132660989)

[When and why is a Threat Analysis performed? 4](#_Toc132660990)

[What are some Existing Threat Analysis Tools? 6](#_Toc132660991)

[The difference between Threat Analysis and Risk Analysis 7](#_Toc132660992)

[Home Security 7](#_Toc132660993)

[Home Network Environment 7](#_Toc132660994)

[Example 1: 8](#_Toc132660995)

[Example 2: 9](#_Toc132660996)

[Example 3: 9](#_Toc132660997)

[Example 4: 10](#_Toc132660998)

[Example 5: 11](#_Toc132660999)

[Threat Analysis on the Home Network 12](#_Toc132661000)

[Existing Home Security Techniques 13](#_Toc132661001)

[Pros 14](#_Toc132661002)

[Cons 14](#_Toc132661003)

[Network Discovery 14](#_Toc132661004)

[What is Network Discovery 14](#_Toc132661005)

[How does Network Discovery work 15](#_Toc132661006)

[Existing Network Discovery Tools 15](#_Toc132661007)

[What are the outputs of Network Security Tools 16](#_Toc132661008)

[Conclusion 18](#_Toc132661009)

[References 18](#_Toc132661010)

# Introduction

In this research report I will talk about the main components of my project, what they are and much more. I will go into detail about the Threat Analysis, what it is, and more. I will also talk about the main home network environments, Home Security and Network Discovery.

# Threat Analysis

## What is Threat Analysis?

Threat analysis is a strategy in cybersecurity to determine which components of an organization, or home’s system needs to be protected and the types of security risks to said system. [[1]](#_References)

By studying and testing the various threats that can be used against an organization in detail, it can allow a security team to gain more information about any threats or vulnerabilities that may be in the wild and even prevent a potential attack before it occurs. The security teams test the threat in real time so they can get more of an understanding of how each attack works and gain a better understanding of the level of expertise that goes into these threats, the exploitation strategies, and the areas in the organisations security that may pose the highest vulnerabilities to these threats.

A Threat analysis is tested against an organization’s own security in real time, categorizing it as a reactive strategy. While the tests are performed against the organizations own defence/security, the amount of damage that could potentially be caused by an unseen cyber-attack can be greatly reduced. [[2]](#_References)

One way to minimize the amount of damage that can potentially be done, is by involving representatives from various groups or departments in an organization to also participate in the analysis and it helps to have multiple perspectives, especially those in specific areas. It is also recommended that the threat analyses take place periodically, such as every year, to allow for any updates, changes or any new threats that may emerge from the changes and growth in technologies. If these threat analyses are done periodically, it can also avoid any previously overlooked threats. [[1]](#_References)

In threat analysis, there are three main categories when it comes to threats, these categories include Accidental Threats, Intentional Threats, and Internal Threats. [[2]](#_References)

**Accidental Threats:** No matter what the error is, whether it is a misconfiguration of a security component of an organization, a mistake in another process or just any accident that can lead to the organization being left exposed is considered an Accidental Threat. These threats are solely caused by human error. By performing a threat analysis, these accidental threats can be identified and mitigated easily before anyone that may want to cause harm can exploit the threat.

**Intentional Threats:** The biggest threat to an organization is the Intentional Threat and it is what is most cause for concern. These threats are conducted by users that mean to cause harm, gain access to or exploit sensitive data for profit. A threat analysis would focus on locating any potential threats that may be on the system already and also to test any that may get onto it in the future.

**Internal Threats:** These types of threats can be a significant cause for concern as most organizations worry about external threats and invest a lot in security to keep those that wish to cause harm out of their systems whereas the real concern for this type of attack is within the company. A prime example of this type of threat may be a disgruntled employee that decides to cause harm to the system in a catastrophic way as it is easier for them to do so with more access and less security.

## What are the benefits of Threat Analysis?

Since the world of technology is always expanding and evolving, as are the threats against them, it is extremely important to stay ahead of these threats. The best way of keeping up to date and ahead of these evolving threats is to constantly look into and study them so that you can have a full understanding on how they work in general and especially on the organizations main network so that it is easy to resolve the issue if it ever arises.

A good and comprehensive Threat Analysis can benefit an organization mostly in many ways, some of the biggest advantages can be that it:

**Saves Money:** A good threat assessment can save a company a significant amount of money, as it allows management or those in decision making positions to determine where to allocate the security resources depending on the department or area that show the highest risk of attack.

**Better Solutions to Threats:** The threat analysis helps with solving a solution to specific threats by understanding the main components of how it works and how it is executed. It is not possible to have a threat analysis set in place if there is not a full understanding of how an attack may work and impede work as it cannot be resolved without prior knowledge.

**Business Efficiency:** A good threat analysis can improve business efficiency, and productivity. It does this because the organizations are much more prepared for meeting their deadlines and achieving their main targets once they are fully aware of the threats that they may face along the way and the best techniques to get around them and resolve the issues if or when they occur. [[3]](#_References)

**Reduce Attack Surface:** If an organization invests in a good, strong Threat Analysis, they benefit from a significant reduction in their attack surface, meaning it will be significantly more difficult for an attacker to cause some damage within the system. This is because if the threat analysis is updated continually, the list of identified threats is also updated. This leads to a significant increase in their security and reducing their attack surface.

**Continuous Updates to Threat Models:** Having up to date threat models are one of the most important aspects of a strong cybersecurity strategy. The Threat Models are meant to show a complex view of the current cyber threats and what they do. Threat Models need to be changed consistently to keep up with the rapid evolution of technology, with every new piece of technology or service that is released to the market there is a potential security risk that cyber criminals aim to exploit. [[2]](#_References)

An up to date risk assessment profile can help with internal audits when assessing the security policies and procedures, and it helps to improve the organizations risk mitigations. The above mentioned show how a good threat analysis is of significant value to an organization that is hoping to improve its security. Assessing threats is a continuous task that calls for constant monitoring of the many parameters of an organization’s operations and how they interact with their environments makes it much easier to mitigate any future attacks or breaches.

## How do you perform a Threat Analysis?

Before you can perform a threat analysis, you must determine the system/ devices the analysis is taking place on. You also must know what a cyber threat is before you can do the analysis.

When performing a threat analysis for an organization, it can be very different or take many different shapes depending on the organization’s specific security requirements. While each threat analysis is different there are four common steps to take when performing a threat analysis that can be found in almost every threat analysis.

The four main steps are:

**Define the Scope of the Threat Analysis:** Any successful Threat Analysis starts with the definition of a scope. Defining the scope of the threat assessment sets the foundation for success by outlining the goals, and more such as what is to be covered in the assessment and what will be required to perform the assessment and ensure its success. Teams must look at what network entities and data they want to protect and define levels of sensitivity for those items to utilize their resources appropriately [[4]](#_References). This whole stage of the Threat Analysis show result in having a clear and direct path or roadmap for what a successful threat assessment will look like, and the steps involved to ensure it.

**Build Processes and Procedures needed to Perform a Threat Assessment:** If there is a proper scope set in place, that defines the goals, what is to be covered and what is the requirements to meet said goals, the overall processes, and procedures should come to fruition. While the scope mentioned above creates the roadmap for the Threat Assessment, the processes and procedures strengthen the approach with tangible tools, processes and the procedures needed to carry out the assessment.

**Implement Policies for data monitoring:** To gather data for a threat analysis, the teams must collect any data from past log data and of any previous incidents such as some phishing attacks, malware infections, port scan attacks and much more. The more vital information would usually come from intrusion attempts, network firewall logs, and other important devices. [[4]](#_References)

**Design a system to Rate the Threats:** Setting up a system to rate the threats that were found in a threat analysis can help understand the severity of each threat, risk, and all vulnerabilities to the organizations stakeholders in an easy to understand format. Creating a threat rating system, that has been agreed upon across the organization and also follows strict rating parameters, can help an organization to report and monitor threats long after the original threat analysis has been performed.

**Perform Threat Analysis:** Once the Scope of the Threat Analysis, the Processes and Procedures that were needed and a system to rate the threats are all put in place, it is time to perform the full Threat Analysis. Organizations can use the expertise of the internal security teams or employees to perform the threat analysis, or they can hire a trustworthy third party organization to perform the threat analysis. [[2]](#_References)

## When and why is a Threat Analysis performed?

While most Threat Analyses are performed on a quarterly basis, a particular organization must base the frequency of their threat analysis based on their own cybersecurity initiatives.

If an organization is based in a high risk area of operation such as the Government, Healthcare or Financial services, then it is required to have a Threat Analysis done more often than other types of organizations. As the need for more Threat Analysis increases, then it would often be more beneficial for the organization to employ a third party to perform the threat analysis as it can use up a lot of the internal resources and may require the hiring of a lot more people to perform the threat analysis. [[2]](#_References)

While the extent and size of the threat analysis can depend on the organization’s size, industry, risk and more, there are several signs to look out for which suggest that the organization may be in need of a threat analysis soon. Some of these particular signs to look out for are:

**Regulatory Compliance Requirements:** The organization might have to meet specific regulatory requirements, for example, there are many rules about testing an organization’s cyber exposure mainly in financial, energy, educational, government and healthcare backgrounds. The compliance starts with a comprehensive cyber threat analysis.

**Your staff isn’t very tech-savvy:** One of the biggest threats to an organization’s cyber security is its internal networks. Any investments in a complex and secure system will go to waste if the employees let anybody in who knocks. While most employees don’t intend to be malicious, they can often be careless or clueless about the security, such as having an unsecure password like, “1234” or “password123” or even clicking on any link that they receive from random emails. Although even those with security awareness training can also fall victim to these issues as they could be too busy to notice a slight change in a colleague or supplier’s email.

**Angry Former Employees:** This depends on the organization and the plans set in place for handling the access of employees that have left or been terminated. Since not all staff leave on good terms it is a good idea to revoke all of their access, change their passwords and remove them from any company systems. Not removing their access is a sure fire way to lead to significant issues in the future.

**Old Technology:** While most organizations don’t like to spend the money to upgrade their systems and if they haven’t experienced any problems, they are not likely to change them any time soon, this technique does not work as well for technology as it would in other circumstances. Old software or operating systems are very likely to expose an organization to greater cyber risks. Once a software reaches a certain age, the provider no longer supports it and no more updates are released, for example with Microsoft and Windows 7, they no longer do big security patches like they would for their newer versions such as Windows 10 or 11. Thinking an old software is safe because there hasn’t been any threats or failures in the system is very dangerous in an organization as there may be some small unnoticed issues and openings that an attacker might notice and exploit. An example of this is the HSE attack as their systems were outdated.

**No data control policies in place:** The amount of entry points in technology is constantly expanding. As well as the organization’s computers, there could possibly be other devices such as laptops, USBs, among others, holding sensitive company data which could be misplaced or stolen. Remote employees could sign into the system from an unprotected network and portable devices that are not encrypted properly. Without policies in place to control the data that flows through the business environment, it can be very difficult to determine the vulnerabilities in an organization by a threat analysis. [[5]](#_References)

## What are some Existing Threat Analysis Tools?

There are many existing Threat Analysis tools for Cyber Security companies, some of which are mentioned in the picture below. These tools are rated based on many different things, such as the Deployment, Behavioural Analytics and much more.

 [[6]](#_References)

**Risk Cloud:** Created by Logic Gate,this is an application that allows you to connect, optimise and scale your Cyber Risk Management Program. Risk Cloud prioritizes cyber risk mitigation and response with Risk Cloud’s Cyber Risk and Controls Compliant Solution. It helps an organization link their cyber risk to their business impact, so they can add context to any risk decision made by reporting what matters most. [[7]](#_References)

**ConnectWise Cybersecurity Management:** When doing my work placement for my third year, I used ConnectWise for everything we did there. It is an easy product to use, and we mostly used it to monitor and secure client devices and servers. They claim to keep a clients infrastructure running and their critical assets secure. Also, with the rapidly evolving technology and the chaos it brings, ConnectWise cybersecurity solutions help MSPs do more with less and make sense of the chaos. [[8]](#_References)

**ManageEngine Firewall Analyzer:** Firewall Analyzer is an agentless log analytics and configuration management software that helps network administrators to understand how bandwidth is being used in their network. Firewall Analyzer is vendor-agnostic and supports almost all open source and commercial network firewalls such as Check Point, Cisco, Juniper, Fortinet, Palo Alto and more. [[9]](#_References)

**WebTitan:** WebTitan is an Advanced DNS Web Security and Content Filtering Software by TitanHQ. WebTitan helps to control the content from the web that an organizations staff access, and it protects the business from online threats with powerful DNS Filtering. It has DNS Security that blocks malware, phishing, viruses, ransomware, and malicious sites at the source. It also has Advanced Threat Intelligence that is a web filter which protects a business and network from malicious web threats in real time. [[10]](#_References)

**Banyan Security:** Banyan Security offers a secure application, infrastructure, and network access, purpose-built for enterprises. Banyan replaces an organizations traditional network appliances, such as, VPNs, bastion hosts, proxies, and gateways, all with a cloud-based zero trust access solution. They offer Networking that is a dead simple setup, with high performance connectivity, it also offers to transfer enterprise security with granular policy controls and also a One click infra access DevOps that never exposes private networks. [[11]](#_References)

That is a small list of some of the companies mentioned in the example picture of the most popular network security tools out there.

## The difference between Threat Analysis and Risk Analysis

While both Threat Analysis and Risk Analysis are an integral part of cybersecurity, there are some differences between the two despite being very similar. Like threat analysis, the goal of risk analysis is to dig deeper into the root processes and the systems to discover any security problems, whereas threat analysis is identifying threats based on security concerns as they happen in real time.

Risk Assessment covers a more broad set of services, applications, policies, and procedures internally that can have an effect on an organization, for example, risk analysis is making sure all of the security systems are working as they should. This is taking a more practical approach than compared to threat analysis, which involves waiting to assess an attack staged against the security tool. [[2]](#_References)

# Home Security

## Home Network Environment

I asked multiple members of my family, friends and even some of the people in my class for a list of devices that would be connected to their home network all of which are below. The lists seem to be remarkably similar with many mobile phones, computers, and other devices such as PlayStation, xbox and more.

There can be a very few minor differences, as some of the examples I have below have some consoles like an Xbox, or a PlayStation and some may have older models, such as PlayStation four or five. Some examples could have different operating systems too, such as PCs or laptops with Windows 11 or 10 and also some with macOS or Linux and even phones being either Samsung, Huawei, or iPhone. There are also some differences, such as some devices being in one house and not another, for example, a Nintendo Switch, ESB Smart meter, Oculus and more.

### Example 1:

##### All Together:

• PC - Windows 11

• ACER Nitro 5 – Windows 11

• ASUS Expert Book – Windows 11

• Govee Light Strips

• 2x Amazon Alexa (4th Generation)

• HP DeskJet Wireless Printer

• 4x Smart TV

• 2x Samsung Galaxy S20

• Huawei Y6 2019

• Samsung Galaxy A22

• Xbox One X

• Xbox One S

• 2x Sky Box

• Oculus Quest 2

• PlayStation 5

• PlayStation 4

• Radio/Speaker

• Vodafone Gigabit Router (connected to NBI, provides Wi-Fi)

• ESB smart meter (outside)

• NBI fibre connection (wired network from the curb)

##### Games Room:

• PC - Windows 11

• Amazon Alexa (4th Generation)

• ASUS Expert Book – Windows 11

• Smart LG TV

• PlayStation 5

• Oculus Quest 2

• Xbox One X

• Samsung Galaxy S20+ Phone

• Govee Light Strips

• HP DeskJet Wireless Printer

##### Sitting Room:

• Smart Samsung TV

• Sky Box

• Vodafone Gigabit Router (connected to NBI, provides Wi-Fi)

##### Kitchen:

• Amazon Alexa (4th Generation)

• ACER Nitro 5 – Windows 11

• Radio/Speaker

##### Bedroom 1:

• Samsung Galaxy A22 Phone

• Smart TV

##### Bedroom 2:

• Xbox One S

• PlayStation 4

• Samsung Phone

##### Bedroom 3:

• Samsung Galaxy S20 Phone

• Huawei Y6 2019 Phone

• Smart TV

• Sky Box

##### Outside:

• ESB smart meter (outside) – connected via SIM to telephone network

• NBI fibre connection (wired network from the curb)

### Example 2:

Paul’s Home Network “Connected Devices” November 2022

• ESB smartmeter (outside)

• HKC home alarm, with WiFi connection to the Internet

• NBI fibre connection (wired network from the curb)

• Vodafone Gigabox Router (connected to NBI, provides WiFi)

• 3 x Gigaset IP phone (base station connected to Gigabox)

• 2 x iMac (2013) running Catalina macOS

• MacBook Air (2022) running Ventura macOS

• MacBook Pro (2015) running Monterey macOS

• MacBook Air (2013) running High Sierra macOS

• Dell Inspiron 15 running Linux (solus)

• Nintendo Wii-U (with WiFi internet connection)

• Nintendo Switch

• 2 x iPhone running iOS 16

• Amazon Echo

• 3 x WiFi-connected Raspberry Pi (with cameras)

### Example 3:

##### All Together:

• Smart Speaker

• Vodafone Gigabit Modem

• Xbox Series X

• MSI Laptop

• 4x Smart TV

• 3x iPhone

• Amazon Alexa

• iPhone

• Xbox One

• Apple Mac

• PC

• Samsung Phone

• PS5

• PS4

##### Sitting Room:

• Smart Speaker

• Vodafone Gigabit Modem

##### Bedroom 1:

• Xbox Series X

• MSI Laptop

• Philips 50" Smart TV

• iPhone

• Amazon Alexa

##### Bedroom 2:

• Smart TV

• iPhone

• Xbox One

• Apple Mac

##### Bedroom 3:

• Smart TV

• PC

• Samsung Phone

• PS5

• Amazon Alexa (4th Generation)

##### Bedroom 4:

• Smart TV

• iPhone

• PS4

### Example 4:

##### All Together:

• PC - Windows 11

• PC - Windows 10

Laptop - Windows 10

2x Smart TV

2x Amazon Alexa

5x Smartphone

PS5

Nintendo Switch

Printer

ESB Smart Meter

NBI fibre connection (wired network from the curb)

Eir Internet Router

Canon Printer

iPad

Govee Light Strips

##### Hallway:

Eir Internet Router

##### Kitchen:

iPad Air

##### Sitting Room:

LG Smart TV

##### Bedroom 1:

Amazon Alexa

iPhone 7

Huwaei P30 Pro

##### Bedroom 2:

PC - Windows 10

Samsung A50

##### Bedroom 3:

PC - Windows 11

Laptop - Windows 10

Govee Light Strip 10m

Amazon Alexa

iPhone 13 Mini

PS5

Sony Bravia Smart TV

Huawei

Nintendo Switch

Canon Printer

##### Outside:

ESB Smart Meter

NBI fibre connection (wired network from the curb)

### Example 5:

##### All Together:

2x PC - Windows 11

2x Laptop - Windows 11

2x PC - Windows 10

2x Smart Light

2x Amazon Alexa

3x Samsung Phone

iPhone

##### Bedroom 1:

PC - Windows 11

Smart Light

Amazon Alexa

Samsung Phone

##### Bedroom 2:

PC - Windows 11

Smart Light

Laptop - Windows 11

Amazon Alexa

Samsung Phone

##### Bedroom 3:

PC - Windows 10

Samsung Phone

##### Bedroom 4:

Laptop - Windows 11

PC - Windows 10

iPhone

## Threat Analysis on the Home Network

The purpose of a Threat Analysis of Smart Homes, or the Home Network was to analyze the smart home and its potential threats. Connected homes powered by the Internet of Things (IoT) have become common. Doorbells, thermostats, locks, and smart appliances have joined streaming video and audio to monitors and speakers throughout our homes. These wired and wireless devices sit inside our home but often connect continuously to remote cloud services. Attackers see these new devices as possible footholds into your home or business, and endpoint protection techniques such as regularly applying security upgrades and enabling operating system security features might not be possible at all times for these new devices. It’s important to be aware of where your sensitive assets and data are stored, and then ensure that the right security controls are in place to protect them. [[12]](#_References)

The research answered questions that were formulated to help potential homeowners and renters make an informed decision to transition from a traditional home to a high-tech smart home. Over the past few decades, the concept of smart home technology has radically evolved with the proliferation of the Internet and homes with connected devices. Similarly, an array of technologies plays an integral part in implementing the Internet of Things (IoT) idea, such as Machine to Machine Communication (M2M), Radio Frequency Identification (RFID), and Near Field Communication (NFC). [[13]](#_References)

M2M communications occur between computers, embedded processors, and mobile devices. The M2M structure consists of five components:

1. The M2M device: Capable of responding to requests for data inside the device.
2. M2M Area Network (Domain of Device): Provides a connection between M2M gateways and M2M devices.
3. M2M Gateway: Utilizes the M2M capability to make sure the devices are interconnecting and inter working in the communication network.
4. M2M Communication Networks (Network Domain): the connection between the M2M application and the gateway(s).
5. M2M Applications: The layer containing middleware where data passes through various application services.

Radio Frequency Identification (RFID) tags identify and track objects in real time through sending and receiving data by means of radio wave transmission. There are two types of RFID tags, these tags are Active and Passive. Active RFID tags use batteries as an independent power source, despite the distance between sensors and tags. These Tags play a large role in conducting inventory counts, increasing accuracy, and saving organizations money in labour costs. Passive RFID tags don’t require a battery to operate, they receive power through electromagnetic signals from the reader inducing a current in the antenna of the tags typically used for toll bridge tags, and debit cards. [[13]](#_References)

Near field communication (NFC) is a wireless communication protocol used in smart devices, access control cards, bank cards and public transportation cards and can be stored on a mobile device. Placing NFC in strategic locations in the home with an interface, central controller, and the devices in the home can be altered by adjusting the temperature when the occupant returns home.

Internet of Things device connections will grow exponentially. While IoT devices continue to become more and more popular, privacy and security are at risk. An attacker can infiltrate a home network undetected and monitor the user’s activity. In addition, IoT devices can be altered by an intruder remotely tampering with the functionality of the devices to launch attacks on the home. An example of this is in 2014, an attack was launched on refrigerators and televisions breaking into over 100,000 consumer devices. [[13]](#_References)

## Existing Home Security Techniques

There are multiple types of existing Home Security; Physical security which would focus more on the physical aspects of the house, such as the entry ways to the household, camera, and other such techniques, an example of a company that prevents this is Phone Watch and Ring Doorbell camera. The primary focus for this report is to focus more on the Network side of security. Some of the existing Home Network Security is already on most of the devices in the household, a good technique to follow when improving the home network security is to keep up with the updates on the software of these devices, removing unnecessary services and software to reduce the attack surface of your network and devices, including your router. Another good technique is to change the default login password and usernames as these can be pre-configured with default credentials to allow an easy setup. When changing passwords, it is critical to use strong and unique passwords to help secure devices. [[14]](#_References)

It can be important to limit access to your wireless network as the more people that have your wireless network credentials, the higher the risk of your data falling into the wrong hands. You can also run up-to-date antivirus software as it is an important protective measure against known malicious threats and can automatically detect, quarantine, and remove various types of malware.

It can also be very important to install a network firewall on all of your network devices. [[15]](#_References)

One very important technique is to regularly back up your data, store it using either external media or a cloud-based service provider that regulates the backup copies of all valuable information residing on your device, it is also advisable to encrypt your backup to protect the confidentiality and integrity of your information.

## Pros

There are a lot more Pros to Home Network Security techniques than Cons, some of these may include:

* While cyber-attacks are not as common in the home as they are for a business, home security measures, such as firewalls and anti-virus software can protect your devices and data from cyber-attacks, including Malwares, Viruses, and hacking attempts.
* A secure home network can help to prevent identity theft by blocking any unauthorized access to your personal information and financial data.
* It can also add the protection for all your devices, home network security can protect any of your devices, including smartphones, laptops, and any other devices in the IoT.
* A very important aspect is the peace of mind it may give a user to have a secure network, knowing that your devices and personal information are protected from potential threats.

## Cons

While there are many pros to home network security measure, there are a few cons, such as:

* The cost is a large con to implementing a comprehensive home network security system as it can be very expensive, more so depending on the equipment and systems used.
* A home network security system can be very complex, setting up and maintaining the security measures would require some IT knowledge.
* Network Performance can also be a big con to a home network security measure, such as the firewalls and content filters can slow down your network performance, especially if you have a large number of devices connected.

# Network Discovery

## What is Network Discovery

The process of Network Discovery allows computers and devices on the same network to find one another. It is the initial step system administrators take when they want to map and monitor their network infrastructure. This process is also sometimes referred to as topology discovery. [[16]](#_References)

As mentioned above, the Network Discovery function is an automatic system search that finds all devices that are connected to the same network, which can then be used to map and monitor the entire network infrastructure automatically. This includes the devices that manage traffic, as well as all the endpoints that are connected to the network. [[17]](#_References)

When connected over a local network, network discovery allows network devices to connect and communicate between other devices that are connected to the same network. This allows system administrators to locate these connected devices easily. With this ability to locate devices quickly on a large network, system admins can then gain a better control over their infrastructure, create device inventories, and enforce better device-access policies. Network Discovery also allows system admins to create network maps, which offer a visual representation of network connections. [[16]](#_References)

Network Discovery is vitally important as many IT teams require visibility into their network infrastructure in order to fulfil their respective duties, they may not be able to understand the relationship between devices and how they communicate with each other when network discovery is not in play. [[18]](#_References)

Hybrid networks, such as wired, and wireless networks can be complicated in a network topology and can therefore make it difficult for IT teams to identify any root causes when an incident or issue occurs, and as digital operations continue to increase in scale, networks are also beginning to change in terms of layout. Therefore, businesses must be able to use network discovery tools to have visibility of all internal activities and devices.

Network Discovery helps in the aid of Cybersecurity, as any invalid IP addresses can be identified as a sign of a malicious device that is carrying malware. IT and Security teams mostly use network discovery to run regular scans to identify threats that might be sitting quietly on a network.

It can also further improve security by helping teams identify open ports on connected devices and inform decisions regarding which ports do and do not need to be open for operations to run effectively. [[18]](#_References)

## How does Network Discovery work

There are three delivery protocols that IT teams use to find and track devices on the network, these are: Simple Network Management Protocol, Link Layer Discovery Protocol, and ping.

* Simple Network Management Protocol (SNMP) lets IT teams gather and organize data about devices on a network.
* Link Layer Discovery Protocol (LLDP) is vendor-neutral and transmits device information to a directly connected device during regular intervals. The neighbouring devices then store this data on management information databases (MIBs) that MSPs and IT teams can access at will. [[16]](#_References)
* Pings are a software utility that lets teams test the reachability of a device on an IP network, they then send an Internet Control Message Protocol (ICMP) to a connected device and measures the time that it takes to receive an answer. [[18]](#_References)

## Existing Network Discovery Tools

There are many Network Discover tools that allow users to scan their network for devices, open ports and more. Some of these tools are covered below:

**Nmap:** Also known as Network Mapper (also with the name Zenmap), it is a free and open-source security tool widely known for its powerful network discovery, enumeration, and security auditing abilities. Network Administrators use Nmap to establish a network map and to get more information about what is going on inside their network, such as which hosts are online, what ports are open, which services are offered, and much more. [[19]](#_References)

**Angry IP Scanner:** Angry IP Scanner or simply ipscan is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports for the devices that is connected to the network, as well as has many other features. It is widely used by network administrators in organizations and also those just curious around the world about network discovery and security, including large and small enterprises, banks, and government agencies. It also works on multiple operating systems, such as Linux, Windows, and MacOS. [[20]](#_References)

**Fing:** Fing is a freemium (Free to use but pay for more options and benefits) network scanner, it Scans your network for all devices connected, it monitors your Internet Speed and security level. One of its Premium feature is to block or pause Internet access on specific devices. It works on multiple operating systems such as Windows, MacOS and also other types of devices, such as a Desktop, Laptop or even mobile. [[21]](#_References)

## What are the outputs of Network Security Tools

Below are screenshots taken of the outputs given from using each of these applications:

Nmap:



Angry IP Scanner:



Fing:



As seen by the images provided, Nmap displays a lot of information about the network and the devices connected to it such as the Devices, IP addresses, MAC Address and more, but is messy and takes time to look through. Angry IP Scanner displays the IP Address, Device Name, and some other information in a much more clear layout. Fing is the most user friendly application, it displays a lot of information about the network and each of the devices connected to it.

# Conclusion

In conclusion, when it comes to a home network security it is very important to perform regular Threat Analyses, also to identify your assets whether it be your banking details or anything else important. It is also recommended to disable any unused ports, installing firewalls on your devices.

A good Network Scanner can be a great help when it comes to a Home Security Threat Analysis as it can help a user, especially any user that may not be Tech Savvy to be able to secure their network. The most recommended application for those not so tech savvy would be Fing, as it displays the devices in a clear layout and allows for more features than most other network scanning tools.

# References

* www.sciencedirect.com. (n.d.). *Threat Analysis - an overview | ScienceDirect Topics*. [online] Available at: <https://www.sciencedirect.com/topics/computer-science/threat-analysis> [[1]](#_What_is_Threat)
* VMware. (2022). *What is Threat Analysis? | VMware*. [online] Available at: <https://www.vmware.com/topics/glossary/content/threat-analysis.html?resource=cat-1112201029#cat-1112201029> [[2]](#_What_is_Threat)
* DisasterRecovery.org. (n.d.). *Threat Assessment | Threat Assessment Plan*. [online] Available at: <https://www.disasterrecovery.org/threat-assessment/> [[3]](#_What_are_the)
* www.solarwinds.com. (n.d.). *Cyberthreat Analysis Tool - Identify Security Threats | SolarWinds*. [online] Available at: <https://www.solarwinds.com/security-event-manager/use-cases/cyber-threat-analysis> [[4]](#_How_do_you)
* Nichols, C. (2020). *7 Reasons to Consider a Cyber Security Risk Assessment*. [online] Cybriant. Available at: <https://cybriant.com/7-reasons-to-consider-a-cyber-security-risk-assessment/> [[5]](#_When_and_why)
* www.capterra.com. (n.d.). *Cybersecurity Software - Review Leading Systems*. [online] Available at: [https://www.capterra.com/sem-compare/cybersecurity-software/](https://www.capterra.com/sem-compare/cybersecurity-software/?utm_source=ps-google&utm_medium=ppc&utm_campaign=:1:CAP:2:COM:3:All:4:US:5:BAU:6:SOF:7:Desktop:8:BR:9:Cybersecurity:11:WCI&gclid=CjwKCAiAyfybBhBKEiwAgtB7fk5jQi_Y-yaTuXgRrxtZXCfxEiAmZmJI82e2JxzYC84fg4HNKu1dKBoCrVsQAvD_BwE) [[6]](#_What_are_some)
* info.logicgate.com. (n.d.). *LogicGate Cyber Risk and Controls*. [online] Available at: <https://info.logicgate.com/capterra-cyber-risk-controls-ub> [[7]](#_What_are_some)
* info.connectwise.com. (n.d.). *ConnectWise Cybersecurity Demo*. [online] Available at: <https://info.connectwise.com/cybersecurity/fortify/demo/sem/cybersecurity-demo?mcid=REV1304&utm_source=capterra&utm_medium=rs&utm_campaign=REV1304&utm_content=demo&loc=na> [[8]](#_What_are_some)
* communications@manageengine.com, M. (n.d.). *Firewall Configuration & Log Management by ManageEngine Firewall Analyzer*. [online] ManageEngine Firewall Analyzer. Available at: <https://www.manageengine.com/products/firewall/?utm_medium=ppc&utm_campaign=Cybersecurity&utm_source=capterra> [[9]](#_What_are_some)
* trust.titanhq.com. (n.d.). *webtitan-web-filter-up 21-01-2022-form*. [online] Available at: <https://trust.titanhq.com/acton/media/31047/webtitan-web-filter-up-21-01-2022-form?utm_medium=ppc&utm_campaign=WT-ENG-Capterra-cybersecurity&utm_source=capterra> [[10]](#_What_are_some)
* www.banyansecurity.io. (2022). *Zero Trust Network Access - Modern VPN - Banyan Security*. [online] Available at: <https://www.banyansecurity.io/?utm_medium=search-paid&utm_source=Gartner_Digital&utm_term=Capterra&utm_content=home_page&utm_campaign=PS-Gartner-Digital-Home-Page&utm_channel=capterra> [[11]](#_What_are_some)
* Mouser.com. (2020). *Assessing Risk on Home Network Security Devices | Bench Talk*. [online] Available at: <https://www.mouser.com/blog/home-network-security-devices> [[12]](#_Threat_Analysis_on)
* www.proquest.com. (n.d.). *Smart Homes: A Threat Analysis - ProQuest*. [online] Available at: [https://www.proquest.com/openview/5352a8a69902425f941d7e583e1eb51f/1?pq-origsite=gscholar&cbl=18750&diss=y](https://www.proquest.com/openview/5352a8a69902425f941d7e583e1eb51f/1?pq-origsite=gscholar&cbl=18750&diss=y%20) [[13]](#_Threat_Analysis_on)
* www.cisa.gov. (n.d.). *Home Network Security | CISA*. [online] Available at: <https://www.cisa.gov/news-events/news/home-network-security>. [[14]](#_Existing_Home_Security)
* Horowitz, D. (2021). *10 Best Ways to Protect Your Home Network Security*. [online] Hp.com. Available at: <https://www.hp.com/us-en/shop/tech-takes/best-ways-to-protect-home-network-security>. [[15]](#_Existing_Home_Security)
* N-able. (n.d.). *What is network discovery?* [online] Available at: [https://www.n-able.com/what-is-network-discovery#:~:text=Network%20discovery%20is%20the%20process](https://www.n-able.com/what-is-network-discovery%23%3A~%3Atext%3DNetwork%20discovery%20is%20the%20process). [[16]](#_What_is_Network)
* Atera - RMM software | PSA & Remote Access for IT Pros. (n.d.). *What is Network Discovery? What you need to know | Atera*. [online] Available at: [https://www.atera.com/what-is-network-discovery/](https://www.atera.com/what-is-network-discovery/%20) [[17]](#_What_is_Network)
* Servicenow.com. (2023). *What is Network Discovery? - ServiceNow*. [online] Available at: <https://www.servicenow.com/products/it-operations-management/what-is-network-discovery.html>. [[18]](#_What_is_Network)
* RangeForce (n.d.). *Network Discovery with Nmap*. [online] RangeForce. Available at: <https://materials.rangeforce.com/tutorial/2019/12/24/Network-Discovery-Nmap/>. [[19]](#_Existing_Network_Discovery)
* angryip.org. (n.d.). *Angry IP Scanner - the original IP scanner for Windows, Mac, and Linux*. [online] Available at: https://angryip.org. [[20]](#_Existing_Network_Discovery)
* Fing. (2021). *Home*. [online] Available at: <https://www.fing.com>. [[21]](#_Existing_Network_Discovery)